ADTRAN n-Command MSP v6.1

Table Of Contents

Getting Started....1
Network Security Considerations....3
Administration Dashboard....4
Administration Dashboard....4
Network Settings....6
Changing Network Settings....7
Date/Time Settings....8
Configuring a Cluster....9
Remote Database....10
Join a Cluster....11
Changing the Administration Dashboard Password....12
System Shutdown/Restart....13
Static Routes....14
Connection Settings....15
Main Dashboard....16
Main Dashboard Tab....16
Average Uptime....18
Current Labels....19
Device Alerts....20
All Alerts....20
Management Alerts....20
Exception Alerts....20

Firmware Alerts....21
Missed Check-In Alerts....21
Operation Alerts....21
Voice Alerts....21
Device Types....22
Heap Usage....23
New Devices....24
Processor Utilization....25
Software Revisions....26
Watch Devices....27
Devices....28
Devices Tab....28
Discovering Devices on the Network....29
Discovering Devices Using a Range of IP Addresses....30
Discovering Devices from an Imported CSV File....32
Preinstalling a Configuration....33
Renaming and Displaying Custom Columns....34
Using Labels....35
Saving Filters....36
Adding Labels to a Device....37
Removing a Device from a Label....38
Removing a Label from the System....39
Discontinuing Management of a Device....40

Changing or Setting Manage Access Parameters....41
Adding New Access Credentials....43
Discovering Devices Manually with Auto-Link....44
Jobs....46
Jobs Tab....46
Toggling Between Jobs Tab Views....48
Creating a New Job....49
Purge Exceptions....51
Pushing Firmware to a Device....52
Pushing a Configuration to a Device....53
Restoring Files....54
Rebooting Device(s)....55
Canceling a Job....56
Deleting a Job....57
Firmware....58
Firmware Tab....58
Uploading Firmware to the n-Command MSP Server....59
Deleting Firmware from the Server....60
Updating Firmware on a Device from the Firmware Menu....61
Alert History and Templates....62
Alert History Tab....62
Alert Templates....63
Adding Criteria to Alert Templates....65

Update Device Alert Settings....66
System Alert Settings....68
Creating an Alert Email Notification....69
Device Details View....70
Device Details Tab....70
Summary Menu....71
VQM Statistics Menu....73
Line Graph....73
Individual Call Detail Grid....74
Backup Files Menu....75
Individual Device Alert Settings....76
SIP Files Menu....77
Exceptions Menu....78
Installing a Configuration File....79
Settings....80
Settings Menu....80
Authentication Settings....81
Local Authentication....82
Radius Authentication....83
LDAP Authentication....84
Active Directory Authentication....86
Setting User Permissions for LDAP or Active Directory Authentication....87
Ignore Devices....89

License Information 90
Log Settings 92
Creating a New Log Entry 93
Editing a Log Entry Notification Type 94
Deleting a Log Entry 95
Login Banner Settings 96
Mail Settings 97
Message Log 98
PCASH Settings 99
Reverse DNS 100
SNMP Settings 101
System Backup 102
Viewing the Available System Backups 102
Creating a Backup Schedule 102
Configuring and Testing the Remote FTP Server Settings 102
System Restart 103
System Updates 104
VQM Statistics Export 105
Users 107
Users Tab 107
Adding a New User 108
Changing a User's Password 110
Editing User Settings 111

Deleting a User....112
Quick Reference....113
n-Command MSP Quick Reference....113
Help Menu....114
About n-Command MSP....115
Edit Account Menu....116
Logout Menu....117
Dashboard Icons....118
Adding a Filter to a List....119
Managing Columns....120
CSV Format Export....121
F.A.Q.....122
n-Command MSP Frequently Asked Questions....122
Why don't I have a Users tab?....123
Why can't I edit a user's jobs and permissions?....124

Getting Started

Welcome to n-Command MSP.

The n-Command MSP server comes preloaded with the n-Command MSP software. The default IP address is **10.10.10.1**. The default login user name is **admin** and the password is **adtran**. There are a few tasks to perform before you can begin using the system to manage devices on your network. For maximum network security, refer to the recommendations in Network Security Considerations.

Log into the n-Command MSP system and complete the following steps to get started:

Step 1. Configure the network settings for your specific network. All the necessary network settings can be configured by accessing **Network Settings** from the **Settings** menu in the upper right corner of the Administration Dashboard. Refer to Changing Network Settings for specific instructions.

Step 2. Generate a new license, if you have not already done so. The system will prompt you to generate a license upon logging into the server for the first time. The license can also be generated by selecting **License Information** from the **Settings** menu in the upper right corner of the GUI. Refer to License Information for detailed instructions for generating the license. You will need to register a user name and password at http://www.adtran.com to access the ADTRAN support website for this step.

Step 3. Change the default admin password. It is strongly recommended that you change the password for the admin account. To change the password, log into n-Command MSP as the **admin** user and select **Edit Account** from the menu bar at the top of the main dashboard. Follow the steps described in Changing a User's Password.

Step 4. Change the Administration Dashboard password. It is strongly recommended that you change the password for the Administration Dashboard. Follow the steps described in Changing the Administration Dashboard Password. Refer to Administration Dashboard to gain access before attempting to change the password.

Step 5. Edit the default device access credentials. One feature of the n-Command MSP software is its ability to automatically discover devices on

your network. In order to successfully discover devices, you must complete two tasks. First, change the default **Device Access** credentials that the system uses to connect with the devices. Navigate to the **Devices** tab and select **Manage Access**. Select the default entry from the list, and make the necessary changes and choose **Save**. Refer to Changing or Setting Manage Access Parameters for more information. Second, enable auto-link on your AOS device. This process is detailed in the *Configuring Auto-Link for AOS* available online at http://supportforums.adtran.com.

Network Security Considerations

For maximum security, n-Command MSP should be deployed in a DMZ behind a firewall. The following considerations should be made to ensure proper operation when deployed in this manner.

Inbound connections are necessary for the n-Command MSP user interface, as well as device management. The following ports should be configured to allow inbound connections for proper operation (inbound traffic can be restricted to management subnets and those containing AOS devices):

- TCP 80 (Auto-link and user interface over HTTP; optional if using HTTPS)
- TCP 443 (Auto-link and user interface over HTTPS)
- TCP 8443 (Auto-link over HTTPS)
- TCP 5060 (VQM reporter; optional if not using VQM reporter)
- UDP 5060 (VQM reporter; optional if not using VQM reporter)
- UDP 161 (SNMP agent; optional if not using the SNMP functionality of n-Command MSP)
- UDP 162 (SNMP trap proxy; optional if not using the SNMP trap proxy functionality of n-Command MSP)

Additionally, the following outbound ports are required to allow access to your configured NTP servers, SMTP servers, and AOS devices:

- UDP port 123 (NTP)
- TCP port 25 (SMTP)
- TCP port 80 (Used to force device check-ins)
- TCP port 443 (Used to force device check-ins)

Administration Dashboard

Administration Dashboard

The **Administration Dashboard** is a graphical user interface (GUI) that provides access to the administrative functions and displays current attributes of the n-Command MSP server. The **Administration Dashboard** is accessible by entering the server's IPv4 address (or host name) into your browser's address field, followed by the path **/msp**.

The dashboard provides real time status for resources on the server, such as **Memory Usage**, **Disk Usage**, and **Server Load**. Depending on the server hardware, additional resource modules may also display, such as **RAID Status**, **Fan Status**, and **System Information**. If your system does not display all the modules explained in this topic, it is because your hardware does not supply that particular information or the server is running on a virtual machine. The following is a brief explanation of the module types and the information each module displays about the server hardware status:

- Memory Usage - Displays the amount of used and available (free) memory.
- Disk Usage - Displays the percentage of hard disk space that is in use and available (free).
- Server Load - Displays a statistical graph displaying the percentage of available RAM, CPU wait time, and load average. The displayed statistics depend upon the options selected. Select one or more of the options from the **Statistics** option at the bottom of the module. The **Data Range** can be set to display by hour, day, week, month, or year.
- RAID Status - Displays the status of each disk in the RAID array. If there is more than one disk array, then the icons are numbered. The color green indicates the device is functioning properly and red indicates a device failure, requiring immediate attention.
- Fan Status - Displays the current status of each fan in the server. The current fan speed is displayed next to the fan name and status in the grid. The color green indicates the fan is functioning properly, yellow indicates a warning condition, and red indicates the fan has failed, requiring immediate attention.

- System Info - Displays the current temperature and power supply status. The color green indicates the device is functioning properly and red indicates a failure, requiring immediate attention.

The resource modules can be manipulated in the following ways:

- To move any of the modules, select the title bar of the module, then drag and drop it to a new location. The other modules will automatically move and realign to accommodate the relocated module.
- To close any of the modules, select the **X** in the upper right corner of the module.
- To add modules to the dashboard, select the **Manage Panels** menu option from the bottom right corner of the dashboard. Select the module to display. Your changes are applied immediately to the dashboard.

The following functions can be performed from the Administration Dashboard:

- Network Settings
- Date/Time Settings
- Cluster Configuration
- Join a Cluster
- Change Password
- System Shutdown/Restart
- Static Routes
- Connection Settings

Network Settings

The **Network Settings** selection of the **Settings** menu (on the **Administration Dashboard**) displays the network configuration. From the dialog box, you can view the **Host Name**, **Default Gateway**, **Primary DNS Server**, and **Secondary DNS Server** settings of the n-Command® MSP server.

Also available from this dialog box are the configurations for each of the unit's Ethernet ports. You can view and edit the Ethernet port's speed and duplex, address type, IPv4 address, and subnet mask. You can also enable or disable the port from this menu.

To change network settings, refer to Changing Network Settings.

Changing Network Settings

To edit the configuration of the n-Command MSP server, follow these steps:

1. Delete the existing information for the server's **Host Name**, **Default Gateway**, **Pri DNS Server** (primary), or **Sec DNS Server** (secondary).
2. Enter the new information in the appropriate fields.
3. Verify the changes have been entered correctly, and select **Apply**.

To change the configuration of an Ethernet port, follow these steps:

1. Select the appropriate Ethernet port tab (for example, **ETH 0**).
2. Make the appropriate changes to the port's enable mode, speed/duplex, address type, IP address, or subnet mask.
3. Verify the changes have been entered correctly, and select **Apply**.

Date/Time Settings

The **Date/Time Settings** selection of the **Settings** menu provides the current server time, the NTP server location, and the time zone. The date and time settings can be changed to suit your particular situation. The NTP server is used to synchronize the time of the local server with a time server. Change the NTP server address by entering a new host name in the **Time Server (NTP)** field. Change the **Time Zone** by selecting an option from the drop-down menu.

Configuring a Cluster

Creating a cluster environment with multiple n-Command MSP servers allows resource sharing across multiple servers and provides an immediately available backup solution. In a clustering scenario with multiple n-Command MSP servers, only one server is configured as the master server, while the others are configured as nodes. The master server allows the nodes to connect to it and provide the same management of network elements as if there were only one n-Command MSP server administering the network. The network elements do not detect nodes, only the master n-Command MSP server. As network elements check in at their various intervals, the master server can redirect them to the other nodes in the cluster environment. All the information about each element is stored in a centralized database that can reside either locally on the master server or remotely on another server.

To configure clustering among multiple MSP servers, complete the following steps:

1. **Designate one of your n-Command MSP servers as the master server. To configure that server,** you must log into the Administration Dashboard of that server.
2. Navigate to the **Settings** > **Cluster Configuration**.
3. Enter the **Cluster Name**, **Bind Address**, **Node Name**, and **Proxy List**. If the database will reside on the local server, do not select the **Remote Database** check box. If the database will reside on a remote server, select the **Remote Database** check box to configure the remote location. (Refer to Remote Database for more information.)
4. Select **Save** to save the settings.
5. Join all nodes to the configured cluster. (Refer to Join a Cluster for more information.)

This process is detailed in *Configuring an n-Command MSP Server Cluster* guide available online at http://supportforums.adtran.com.

Remote Database

To configure a remote database, use the expanded menu that displays when you select the **Remote Database** check box from the **Cluster Configuration** dialog box.

1. Enter the **Database Host**, **Port**, **User**, and **Password** credentials for your remote PostgresSQL database.

Database Host	The address of the remote database server. Specify as either IPv4 address or host name.
Port	The port on which the database is listening. The default port for PostgresSQL is **5432**.
Postgres User	The user name used to log into the database to initialize the schema. The default user name is **postgres**.
Postgres Password	The password for the user.

2. Optional. Connectivity to the remote database can be tested by selecting **Test Connection**. By testing the availability of the remote server, you are also testing the authentication as well.
3. Select **Save** to save these settings.
4. You are prompted to initialize the database schema on the remote server. Upon confirmation, the database will initialize and the application will restart.

In order to use a remote database, the remote database server must be configured prior to configuring the n-Command MSP master server.

Return to Configuring a Cluster.

This process is detailed in *Configuring an n-Command MSP Server Cluster* guide available online at http://supportforums.adtran.com.

Join a Cluster

In order for a node to join a cluster, the cluster must already be configured using steps described in Configuring a Cluster. Follow these steps to join a cluster:

1. Log into the **Administration Dashboard** of the node server you want to add to the cluster.
2. Navigate to the **Settings** > **Join Cluster**.
3. Enter the necessary settings for Cluster Host, Bind Address, Username, and Password.

Cluster Host	The host name or IPv4 address of the master server in the cluster you are joining.
Bind Addres:	The IPv4 address of the node you are adding to the cluster.
Username	The user name for the master server you are joining. The default is **admin**.
Password	The password for the master server you are joining. The default is **adtran**.
These credentials are the same as the login information for the Administration Dashboard login.	

4. Select **Find Cluster** to locate the cluster. If the search is successful, the **Node Name** field displays at the bottom of the **Join Cluster** dialog box. The field is blank and you will enter the name in the next step.
5. Enter a name for the node you are adding to the cluster. Use a unique name to identify it from other nodes. Select **Join Cluster** to save the configuration and restart the application. This may take a few minutes to complete. Once finished, the node will be successfully added to the cluster.

Repeat these steps for any additional nodes that need to be added to the cluster, supplying a unique name for each.

This process is detailed in *Configuring an n-Command MSP Server Cluster* guide available online at http://supportforums.adtran.com.

Changing the Administration Dashboard Password

You can change the password once you are logged into the **Administration Dashboard**.

1. Navigate to **Settings** > **Change Password**.
2. Enter your current password.
3. Enter the new password.
4. Re-enter the new password in the **Verify** field.
5. Select **Save** to save the new password and exit the dialog box.

*The administration dashboard user name and password is independent of the main dashboard user name and password. The default user name is **admin** and the default password is **adtran**.*

If this is your first time accessing the administrative dashboard after upgrading from a version prior to 5.1, the password is the serial number of the server.

System Shutdown/Restart

The **System Shutdown/Restart** option on the **Settings** menu of the **Administration Dashboard,** allows you to shut down the server, restart the n-Command MSP application, or reboot the server.

- Select **Shutdown** to power down the server.
- Select **Reboot** to power down the server and restart.
- Select **Restart Service** to restart the n-Command MSP application service without powering down the server.

Select **Cancel** to exit the dialog box without performing any of these functions.

Static Routes

The **Static Routes** option on the **Settings** menu of the **Administration Dashboard** provides a menu for configuring static routes. A static route is configured by specifying an interface, destination IPv4 network, subnet mask, and gateway. Existing static routes can be deleted from this menu as well.

Connection Settings

The **Connection Settings** option on the **Settings** menu of the **Administration Dashboard** provides a way to view and modify the Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS) ports used by n-Command MSP. From this dialog box, you can view the port settings of the n-Command MSP server. Changes can also be made to any of these settings by editing the information in the provided fields and selecting **Save**.

Main Dashboard

Main Dashboard Tab

The main **Dashboard** tab is the first menu to display after logging into the system. It provides real time status for all devices being managed by the system using the **Average Uptime**, **Current Labels**, **Device Alerts**, **Device Types**, **Heap Usage**, **New Devices**, **Processor Utilization**, **Software Revisions**, and **Watch Devices** modules. Each of the modules can be closed, resized, or moved around within the screen. They can also be customized to display data by device type, group, or firmware version by modifying the options settings.

The following are some common tasks related to the modules view:

- To move any of the modules, select the title bar of the module and drag and drop it in its new location. All of the other modules will automatically move and realign to accommodate the moved module.
- To close any of the modules, select the **X** in the upper right corner of the module.
- To resize the modules, select the maximize/minimize icon to toggle between these two views. If there are many devices being managed, this is a very helpful tool to view all the data available in a module.
- To open modules on the dashboard, select the **Manage Panels** menu option from the bottom right corner of the dashboard. Select the module to display. Your changes are applied immediately to the dashboard. Multiple instances of the same module can be displayed on the dashboard at the same time. Close the menu by selecting the **X** in the upper right corner.
- To filter the devices displayed in the modules, select the **Filter** option from the bottom right corner of the dashboard. All saved filters will display in this menu. Select the filter to use and the dashboard updates accordingly. To remove the filter, select the **Filter** option again and select **None** from the menu. More information about saving filters is available in the section Saving Filters.

Use the following links for more information on each module:

- Average Uptime
- Current Labels
- Device Alerts
- Device Types
- Heap Usage
- New Devices
- Processor Utilization
- Software Revisions
- Watch Devices

Average Uptime

The **Average Uptime** module on the **Dashboard** tab displays the average number of days the devices have been operational. This module can be filtered to show only those devices with a maximum or minimum uptime specified in the options settings. The **Refresh** rate can also be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

The devices are grouped together by platform type. For instance, all the NetVanta 7100s are grouped together and all the Total Access 916 Gen 2 are grouped together. For more detailed information about a device type, click on the column. This breaks the data down further by the firmware revision. For an even more detailed view, double click the firmware column. This opens the **Devices** menu with a filter for the specific firmware applied.

Current Labels

The **Current Labels** module on the **Dashboard** tab displays labels created in the system. The **Refresh** rate can be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

This module also provides a quick link to the **Devices** menu with the label applied as a filter. To display the units assigned to a particular label in the **Devices** menu, double click the representative portion of the chart.

Device Alerts

The **Device Alerts** module on the **Dashboard** tab displays all alerts present throughout the system. The system reports alerts for **Management**, **Exception**, **Firmware**, **Missed Check-Ins**, **Operations**, **and Voice** errors. The alert notices can be filtered or sorted by the alert type. The icons above the columns change to display a red warning box with the number of errors detected when alerts of that type exist in the system. Choose the desired alert type icon to display more information on the grid. The information provided depends on the alert type. Double click on the device listed in the grid for more specific details about a particular device. This action opens the **Device Details** menu.

The order in which the icons are presented on the Dashboard can be altered through the options settings. Select the wrench in the lower right corner of the module. Select the alert icon next to **Order**, and drag the icon to the new position and drop into place You can continue to drag and drop the alert icons in any order in which you want them to appear.

The **Refresh** rate can be changed from 30 seconds to 1 or 5 minutes, also through the options settings. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

All Alerts

Choose the **All Alerts** icon to view all the alerts together. To sort the alerts by one of the column headings, click any column. The order changes from ascending to descending with each additional click.

Management Alerts

Management alerts are issued when a device's auto-link is disabled or the running configuration has not been saved to the startup configuration. When filtered by **Management** alerts, the dashboard grid displays the device name and a check-mark to indicate an unsaved configuration or disabled auto-link in the appropriate column.

Exception Alerts

Exception alerts are issued when an exception file is present on the device. When filtered by Exception alerts, the dashboard grid displays just the device name and the number of exceptions on the device. Double clicking on the device

listed provides detailed information about the exception by jumping to the **Exceptions** tab in the **Detailed Device** menu.

Firmware Alerts

Firmware alerts are issued when a primary or backup firmware image is not on the system, the currently executing firmware version is not the same as the primary firmware image, or the specified primary and backup firmware images are the same file. When filtered by Firmware alerts, the dashboard grid displays the device name, and a check-mark to indicate as to whether the primary, backup, and running firmware are presently running. The grid also displays a check-mark if the primary and backup firmware are the same.

Missed Check-In Alerts

Missed Check-In alerts are issued when a device misses the most recently scheduled check-in with the n-Command MSP server.

Operation Alerts

Operation alerts are issued when a device experiences a warm start, cold start, authentication failure, low nonvolatile RAM, and low CompactFlash memory.

Voice Alerts

Voice alerts are issued when a SIP device experiences a low mean opinion score (MOS) or fails to register.

Device Types

The **Device Types** module on the **Dashboard** tab depicts the devices by type in a pie chart. The pie chart can be changed to show the devices by group as well through the Options Settings. The **Refresh** rate can also be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

For more detailed information about the devices, double click on the chart. This opens the **Devices** menu with a filter for the specific device type or group applied.

Heap Usage

The **Heap Usage** module on the **Dashboard** tab displays the percent of heap used on each device. This module can be filtered to show only those devices with a minimum change or minimum usage by specifying a value in the options settings. The number of devices can be limited by setting the **Max Devices** number, up to 100 devices. The **Refresh** rate can also be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

For more detailed information about a particular device, double click the device in the grid. This opens the **Device Details** menu.

New Devices

The **New Devices** module on the **Dashboard** tab displays all the new devices discovered on the network in the last 10 days. The **Refresh** rate can be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

For more detailed information about the new devices, click on the column. A grid displays the device type, number of devices added, and the percentage of the whole group these devices make up. Updates are not provided while in the detailed view. The refresh interval only applies to the summary view.

Double click on a row in the grid to go to the **Devices** tab. A filter for the device group and date added are already applied to the resulting list of devices.

Processor Utilization

The **Processor Utilization** module on the **Dashboard** tab displays the percent of processor being used on each device. This module can be filtered to show only those devices with an minimum usage by changing the options settings. The number of devices can be limited by setting the **Max Devices** number. The **Refresh** rate can also be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

For more detailed information about a particular device, double click the device listed in the grid. This opens the **Device Details** menu.

Software Revisions

The **Software Revisions** module on the **Dashboard** tab depicts the software revisions in a pie chart. The view can be adjusted to show just the **Primary**, **Backup**, or **Running** firmware versions by changing the options settings. The **Refresh** rate can also be changed from 30 seconds to 1 or 5 minutes. The options settings are available by selecting the wrench in the lower right corner of the module. After making changes to the options, select the wrench again to return to the status view.

For more detailed information about the devices, double click on the chart. This opens the **Devices** menu with a filter for the specific firmware applied.

Watch Devices

The **Watch Devices** module on the **Dashboard** tab is a group of devices that match a specified filter. By selecting the wrench in the lower right corner of the module, you can specify a filter to use and also customize the display settings. You can only choose one filter at a time to display in the **Watch Devices** module. The list of filters displayed reflects any filters already created and saved within the system. For information on creating and saving filters, refer to Adding a Filter to a List and Saving Filters.

The displayed results can be limited to a maximum number of devices through the display settings. You can also change the sort criteria, sort order, and the refresh rate. After making changes to the options, select the wrench again to return to the status view with the changes in effect.

From the status view displaying the watched devices, there are additional features available. You can export the list to a CSV file using the Export CSV option in the lower left corner or change the columns displayed using the Manage Columns option in the lower right corner. These features are explained in the **Related Topics** below.

Devices

Devices Tab

The **Devices** tab allows you to discover devices on the network, preinstall configurations, group the devices by type, add labels, discontinue device management, and edit Manage Access parameters. To open the **Devices** tab, select the **Open Tab** menu from the upper left-hand corner of any screen in n-Command MSP. Select **Devices** from the drop-down menu.

The number of managed devices displayed on the Devices tab can be limited to 20, 30, 50, 100, 500, or 1000 devices per page using the **Page Size** menu at the bottom of the page. The display settings can also be set to automatically choose the number of devices to fit on the page (select **Auto**) or to display all devices (select **All**). Choosing to display **All** devices could cause a delay in the amount of time it takes to refresh the screen if there are a large number of managed devices. Use the navigation tools at the bottom of the page to view additional pages. By default, the devices are displayed to automatically fit the page and are sorted by the **Hostname** column.

To find out more information about specific tasks available from this menu, select from the following:

- Discovering devices on the network
- Preinstalling a configuration
- Renaming and displaying custom columns
- Using labels
- Discontinuing management of a device
- Changing or setting Manage Access parameters

Discovering Devices on the Network

n-Command MSP can manage AOS devices located on the network once they have been discovered. The discovery process locates devices running AOS versions A2.04, 17.05.04, or later. There are two methods for discovering devices. Use one of the following links for instructions:

- Discovering Devices Using a Range of IP Addresses
- Discovering Devices from an Imported CSV File

Discovering Devices Using a Range of IP Addresses

A group of devices can be discovered all at once using an IP address range. By providing the beginning IP address and the ending IP address (or subnet mask), n-Command MSP can identify all devices within the range capable of being managed. Use the following steps to discover devices on the network using this method:

1. Navigate to the **Devices** tab at the top left of the menu.
2. Select **Discover Devices** from the **Manage** drop-down menu.
3. Select the IP address that the discovered device will use to access the server from the **Select An Interface** drop-down menu. Each server has four ports, enabling it to be connected to four different networks.
4. Enter the **Contact Interval** to assign to the successfully discovered devices. This interval is the delay time (in seconds) between each attempt of the device to check-in with the server.
5. Select the connection method to use, either **HTTP** or **HTTPS**.
6. Enter the beginning IP address to start searching, in the **Start IP Address** field.
7. Enter the ending IP address to complete the range, or enter a subnet mask in the **End IP or Subnet Mask** field.
8. Select the **Authentication** for user name and password usage. If the appropriate entry is not listed, select **Edit** and follow the steps explained in *Adding New Access Credentials*.
9. Choose **Start** to begin the discovery process. (If the **Start** button is not available for selection, it could be because not all of the necessary information was provided. Go back through the fields and data selection steps to make sure all entries are provided.)
10. A job is created to discover the devices using the criteria provided. The status is shown in the **Jobs** tab menu. All devices located in the IP address range meeting the requirements to communicate with the server, will now appear in the **Devices** tab menu.

Devices that are configured to report to a different n-Command MSP server are not reconfigured to report to this one.

Discovering Devices from an Imported CSV File

Devices can be discovered by importing the necessary information from a comma separated value (CSV) file. The CSV file should list the following information: **IP Address**, **Username**, **Password**, **Method** (HTTP/HTTPS), and optionally **Port Number**. Use these steps to discover devices and add them to the **Devices** tab for management:

1. Navigate to the **Devices** tab at the top left of the menu.
2. Select **Discover Devices** from the **Manage** drop-down menu.
3. Select the interface to use to access the network from the **Select An Interface** drop-down menu. Each server has four ports, enabling it to be connected to four different networks.
4. Enter the **Contact Interval** to assign to the successfully discovered devices. This interval is the delay time (in seconds) between each attempt of the device to check-in with the server.
5. Select the **CSV File** tab.
6. Choose **Browse** to locate the CSV file.
7. Once the file is located, choose **Open**. The information in the selected file will be uploaded to the **Discover Devices** grid.
8. Select **Start** to begin the discovery process.

Once the devices are discovered, they will populate the **Devices** tab menu.

Preinstalling a Configuration

The **Preinstall Config** feature allows a customized AOS configuration file to download to a device as soon as it is discovered. Prior to deploying a device in the field, the configuration file is generated and uploaded to n-Command MSP along with the serial number of the device. Once the device is installed and discovered, the preinstalled configuration file is downloaded to the device, overwriting the current configuration, and rebooting the unit.

1. Navigate to the **Devices** tab by selecting **Devices** from the **Open Tab** menu in the upper left-hand corner of the screen.
2. Select **Preinstall Config** from the **Manage** drop-down menu, also in the upper left-hand corner of the screen.
3. Enter the **Serial Number** of the device.
4. Enter the configuration file name in the **Config File** field or select **Browse** to find a file locally or on the network.
5. Optionally, select **Save on Reboot** to save the running configuration as the startup configuration on the device.
6. Select **Preinstall** to complete the task.

Renaming and Displaying Custom Columns

There are five custom columns provided in the n-Command MSP server. These custom columns can be renamed and displayed on the **Devices** tab.

1. Select **Rename Custom Columns** from the **Manage** drop-down menu.
2. Enter the new column name in the fields provided.
3. Select **Save** to save the settings and return to the **Devices** tab.
4. To display the columns, choose **Columns** from the bottom right corner of the Devices tab. Select the columns you want displayed by the check box next to the column name.
5. Select the **X** in the upper right corner when finished to close the menu.

Using Labels

All of the managed devices can be grouped in a number of ways to make better use of the dashboard modules and maintenance tasks. This is accomplished by creating labels to identify the group and adding devices to the label. The following sections explain how to add a label, add devices to the label once it is created, remove devices from the label, and delete a label from the system. Use the following links for more information:

- Adding Labels to a Device
- Removing a Device from a Label
- Removing a Label from the System

Grouping by labels basically adds a label to the device, allowing it to display when the label group is chosen. Devices can belong to more than one label at a time. If a device is removed from the label, the device is not being removed from the system. A device that has not been added to any label will still display when the **All Devices** or **Unlabeled Devices** category is selected. The **Unlabeled Devices** is a default group containing all devices that have no label assigned to them.

Additionally, a filter can be added to further limit the devices displayed from within a label. Filters are selected from the drop-down menu under **Saved Filters**.

To create a filter and save filters, refer to the following sections:

- Adding a Filter to a List
- How to Save a Filter

Saving Filters

Filters are used to limit the devices displayed in a list based on a specified criteria. To create a filter in the **Devices** tab, refer to Adding a Filter to a List. To save the filter once it is applied, use the following steps:

1. Select the **Add** button under the **Saved Filters** heading.
2. Enter a descriptive title for the filter in the blank field provided.
3. Select **Add** to save it.

The filter will apply automatically to new devices as they are discovered. The filter title can be changed using the **Edit** feature from this same menu. Select the filter from the drop-down menu and select **Edit**. Make the necessary changes and save it again.

Delete a filter by selecting it from the drop-down menu and select **Delete**. The filter is removed from the list.

Adding Labels to a Device

Use the following steps to create labels and add devices:

1. From the **Devices** tab, enter a new label name in the **Labels** field.
2. Select **Add** (or press Enter) to create the label and add it to the list below **All Devices**.
3. Select the devices to add to the label and drag them to the new label. The icon changes as it is being dragged. When the device is directly on top of the label and shows a green + sign, drop it into the label group. Continue to drag and drop devices into the label group until all are present. You can also drag multiple devices at one time by selecting all devices first, then dragging the group to the label.

Removing a Device from a Label

Use the following steps to remove a device from a label:

1. From the **Devices** tab, select a label to list the devices associated with it.
2. Select the device from the list on the right. The **Remove from Label** option above should become available in the taskbar directly above the device list.
3. Select the **Remove from Label** option. The device will be removed from the label and no longer appear in the list to the right of the label listing.

Removing a Label from the System

A label can be removed completely from the system. The devices which were included in the label remain in the **All Devices** group, as well as in any other label containing them. Use the following steps to remove a label from the system:

1. From the **Devices** tab, select the label to be removed from the list on the left side of the menu.
2. Select the minus circle button that appears next to the label. The label is deleted.

The label can be renamed by double clicking it and typing a new name in the field provided.

Discontinuing Management of a Device

Devices can be deleted from n-Command MSP so they are no longer actively managed by the system.

1. From the **Devices** tab, select **All Devices**.
2. Locate the device to be removed in the list on the right. Select the check box next to the device.
3. Select **Delete**. The device is removed from the system and no longer being managed.

	Some devices will continue to check in with the server based on the parameters set on the device itself. It may be necessary to make changes to the AOS settings on the local device as well, to keep it from automatically linking with the n-Command MSP server.

Changing or Setting Manage Access Parameters

Manage Access parameters provide the access credentials (user name and password), as well as the preferred IP address, port, and method for connecting to the device from n-Command MSP. Each set of parameters can be managed in a central location and applied to any number of devices on the network.

Use the following steps to add a new set of Manage Access parameters:

1. From the **Devices** tab, select **Manage Access** from the menu.
2. Select **New** from the **Device Access** dialog box.
3. Select the text in the **Name** field and enter a new name for this item.
4. Select the **Access Credentials** from the drop-down menu. If the credentials needed are not listed, refer to Adding New Access Credentials to create a new set.
5. Select the **IP Address** check box if a specific IP address needs to be supplied and enter the IP address in the blank field provided. If this is not necessary, skip to Step 7.
6. If necessary, enter the port number to use.
7. Select the **Method** to use, either **HTTP** or **HTTPS**.
8. Select **Save** to add the new parameters.

Additional tasks can be performed from the **Device Access** menu, such as changing the default, removing a set of parameters, or editing them as necessary.

- To change the default parameters, select the set of parameters from the list on the left and choose **Set Default**. Only one set of parameters can be used as the default. There must always be one set of parameters set as the default, and the default cannot be deleted.
- To delete a set of parameters, select the name of the access parameters from the list on the left and select **Delete**. Confirm the prompt by choosing **Yes**.

- To edit a set of parameters, select the name of the access parameters from the list on the left and make the necessary changes. Select **Save** once the all changes are completed.

Adding New Access Credentials

When discovering devices, an authentication user name and password must be entered to allow access to the device. These are called Access Credentials and can be managed by the system. New entries are added from the **Discover Devices** menu by selecting the **Edit** button or from the **Manage Access** dialog box by selecting **Manage Credentials**.

Use the following steps to add a new entry:

1. Select the **+** (plus) button on the lower left side of the menu to add a new entry.
2. Enter the user name, password, and a description to help identify the entry in a list.
3. Select **Save**.

Additional tasks can be performed from the **Discover Devices** menu. Entries can be removed or edited as necessary.

- To remove an entry, select the entry from the list (only one selection can be made at a time) and choose the **-** (minus) button from the bottom of the menu. Choose either **yes** or **no** to confirm the action.
- To edit an entry, select the entry from the list, and choose the **Edit** button from the bottom of the menu. Make the necessary changes to the entry and choose **Save**.

Discovering Devices Manually with Auto-Link

Devices can be discovered manually by configuring the auto-link settings on the AOS network products. Connect to the device through console, Telnet, or secure shell (SSH) as described in the quick start guide that shipped with the unit or available online at http://www.adtran.com. Once auto-link is enabled and configured on the device, it will check in with the server and become a managed device. Enter the following configuration in the command line interface (CLI):

1. Enter the n-Command MSP server IP address to manage the device:

    (config)**#auto-link server** <*ip address* | *hostname*>

    *w*here <*ip address* | *hostname*> is the host name or IP address of the MSP server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

2. Optionally specify the interval (in seconds) between attempts to contact the n-Command MSP server:

    (config)**#auto-link recontact-interval** <*value*>

    By default, the AOS device will contact the server every **3600** seconds. A recontact interval of less than 3600 seconds is not recommended. Specifying an interval of **0** seconds disables the recontact feature.

3. Enable auto-link on the AOS device by entering the **auto-link** command from the Global Configuration mode prompt.

    For example,

    (config)**#auto-link**

Additional information about configuring the auto-link feature on the AOS device is available in the configuration guide *Configuring Auto-Link for AOS and n-Command MSP*, available online from the ADTRAN Support Forum at http://supportforums.adtran.com.

Additional information about these commands and using the CLI is can be found in the *AOS Command Reference Guide* available online at http://supportforums.adtran.com.

Jobs

Jobs Tab

The **Jobs** tab enables you to create, edit, and manage specific jobs you want to perform on your network. The jobs included are **Push Firmware**, **Push Configuration**, **Restore**, **Reboot**, and **Purge Exceptions**. Each user on the network is configured to have access to specific jobs, or all jobs, depending on their user configuration. The network administrator is responsible for configuring the user's permissions. For more information, refer to Adding a New User. Each job can be applied to a single managed device or a group of managed devices, and each job can be configured to run on a schedule.

To open the **Jobs** tab, select the **Open Tab** menu from the upper left-hand corner of any screen in n-Command MSP. Select **Jobs** from the drop-down menu.

There are two available views of the main **Jobs** tab: the **Details** view and the **Grid** view. You can toggle between views by selecting either the **Details** or **Grid** button from the top right corner of the menu.

The **Details** view gives the details of each currently configured job. Currently configured jobs are listed on the left side of the menu, and details for each job are provided in the split screen to the right. To access details for different jobs, select the job title from the list on the left. Some of the information displayed is the job's status, start and end times, percent completion, and number of errors.

The **Grid** view of the **Jobs** tab lists the currently configured jobs. This list includes the **Job Name**, **Description**, **Status**, job **Start Time**, and the **User** that created the job. This list can be exported via comma separated value (CSV), and the columns in the list can be managed by the **Manage Columns** tab at the bottom right side of the list. Jobs can also be deleted or cancelled from the **Grid** view by selecting the box next to the job and then selecting **Cancel** or **Delete** from the top of the **Jobs** tab.

From the main **Jobs** tab, you can view your currently configured jobs, add a new job, cancel a job, and delete a job. For more information on common job tasks, select a topic from the following list:

- Toggling Between Jobs Tab Views

- Creating a New Job
- Pushing Firmware to a Device
- Pushing a Configuration to a Device
- Restoring Files
- Rebooting Device(s)
- Canceling a Job
- Deleting a Job

Toggling Between Jobs Tab Views

To toggle between the **Details** and **Grid** views of the **Jobs** tab, follow these steps:

1. For the **Details** view, select the **Details** button on the top right corner of the **Jobs** tab.
2. For the **Grid** view, select the **Grid** button on the top right corner of the **Jobs** tab.

You can toggle back and forth between views as often as necessary.

Creating a New Job

To create a new job from the **Jobs** tab, select the **Schedule Job** button at the top left of the menu. Selecting this button opens a new window, entitled **Schedule New Job**. In the **Schedule New Job** window, there are five sections (**Targets**, **Tasks**, **Schedule**, **Notifications**, and **General**) that display down the left side to guide you in configuring the job. Enter the information for each section as described in the steps below. All sections must be completed before the **Create Job** button will become available to create the configured job. To begin configuring the job, follow these steps:

As you enter the information for each tab of the new job, the tab will display either a green check mark or a red X in the right corner. The green check mark indicates that the tab has been filled out completely and is ready for processing. The red X indicates that the tab is partially defined and that the job cannot be initiated until all the information is entered or until an invalid entry is corrected. If neither a green check mark nor a red X appear, the tab has not been addressed.

1. Select the devices to target for the job in the **Targets** section. You can specify that the job will run on all devices by selecting the check box for that option, or you can select specific devices from the **Devices**, **Labels**, and **Filters** tabs. Devices are selected by checking the box next to the appropriate device, then dragging them to the screen below. Multiple devices can be selected at one time and dragged simultaneously to the **Devices for Job** screen at the bottom of the page. Select **Next** to continue to the next step or select **Tasks** from the list.

If you are upgrading firmware, all selected devices must be the same type of device. For example, all NetVanta 7100s or all Total Access 900s.

2. Select the **Tasks** section to configure the new job's tasks. You can select from **Reboot**, **Restore**, **Push Configuration**, **Push Firmware**, or **Purge Exceptions**. Select the tasks you want completed in this job by checking the box next to the appropriate tasks. You will be prompted for more information about each task

you select. For more details about each task, select the task from the following list:

- Purge Exceptions
- Pushing Firmware to a Device
- Pushing a Configuration to a Device
- Restoring Files
- Rebooting Device(s)

3. Select the **Schedule** section to configure the new job's schedule. You can specify whether the job will start at a specific time or immediately, by selecting the appropriate option. If you want to specify a start time, you can enter the date and time. From this tab, you can also specify the job's maximum run time by entering the hours and minutes of job duration. Select **Next** to continue to the next step or select **Notifications** from the list.

4. Select the **Notifications** section to select the event you want to trigger a notification (job completion, job completion with error, or first error), and whether or not detailed log information will be included in the notifications. You can define the users who will receive email notifications either by choosing a user from the list or entering email addresses. Select **Next** to continue to the next step or select **General** from the list.

5. Select the **General** section to enter the name of the job and the job's description. For example, you might enter **Firmware Upgrade** in the **Name** field and **A2 Firmware** in the **Description** field.

6. When all necessary requirements have been completed, select **Create Job** from the top right of the menu.

	*If the **Create Job** button is not available, it could be because not all the necessary requirements have been completed. Check each of the five sections for completion.*

Once all the sections are complete and **Create Job** has been selected successfully, the job will start at the time you specified.

Purge Exceptions

A new job can be created to purge all exception alerts on a device. Once the exception alerts are cleared from the device, the exception condition is cleared from n-Command MSP as well. To create a **Purge Exception** job, navigate to the **Schedule New Job** menu by selecting **Schedule Job** from the **Jobs** tab. Refer to Creating a New Job for information on creating a new job. You will assign the task as **Purge Exceptions**.

Pushing Firmware to a Device

Navigate to the **New Job** window by selecting **Add Job** from the **Jobs** tab. Select the **Tasks** tab from the **New Job** window. Refer to Creating a New Job for more information on accessing the **New Job** window and configuring notifications, schedules, and devices that accompany this job.

Once you are in the **Tasks** menu, select **Push Firmware** to configure the firmware push. To configure this job, follow these steps:

1. Specify the **Device Group** whose firmware you want to upgrade. You can choose the device group from a drop-down menu of all your currently configured groups.
2. Specify the **New Firmware** to which you are upgrading. You can choose the firmware from a drop-down menu of all your currently loaded firmware.
3. Specify whether the unit's configuration will be saved to the unit's nonvolatile random access memory (NVRAM) by checking the check box next to **Write Config**.
4. Specify the **Firmware Destination** from the drop-down menu. You can select **Automatic** (default), **CFLASH**, or **NONVOL**.
5. The **Push Firmware** task configuration is now complete.
6. You can now return to configuring additional parameters for this job or other tasks to accompany this job as described in Creating a New Job.

Pushing a Configuration to a Device

Navigate to the **New Job** window by selecting **Add Job** from the **Jobs** tab. Select the **Tasks** tab from the **New Job** window. Refer to Creating a New Job for more information on accessing the **New Job** window and configuring notifications, schedules, and devices that accompany this job.

Once you are in the **Tasks** menu, select **Push Config** to push a configuration to a unit, or units, managed by n-Command MSP. To configure this job, follow these steps:

1. Enter the configuration into the **Push Configuration** dialog box. This information can be entered manually, or copied and pasted from a text file.
2. Select whether you want to save the unit's configuration before pushing the new configuration, or after pushing the new configuration by checking the appropriate check box.
3. The **Push Configuration** task is now complete.
4. You can now return to configuring additional parameters for this job or other tasks to accompany this job as described in Creating a New Job.

Restoring Files

Navigate to the **New Job** window by selecting **Add Job** from the **Jobs** tab. Select the **Tasks** tab from the **New Job** window. Refer to Creating a New Job for more information on accessing the **New Job** window and configuring notifications, schedules, and devices that accompany this job.

Once you are in the **Tasks** menu, select **Restore** to configure the file restoration job. To configure this job, follow these steps:

1. Enter the date closest to the backup files you want to restore on the unit. The date can be entered manually, or by selecting the date on the calendar.
2. Enter the time closest to the backup that created the files you want to restore on the unit. You can enter the time manually, or by scrolling with the **up** and **down** arrow keys.
3. Select whether or not you would like to restore this unit from another device by selecting the appropriate check box. You can choose the device you would like to use as a backup from the drop-down menu.
4. The **Restore** task is now complete.
5. You can now return to configuring additional parameters for this job or other tasks to accompany this job as described in Creating a New Job.

Rebooting Device(s)

Navigate to the **New Job** window by selecting **Add Job** from the **Jobs** tab. Select the **Tasks** tab from the **New Job** window. Refer to Creating a New Job for more information on accessing the **New Job** window and configuring notifications, schedules, and devices that accompany this job.

Once you are in the **Tasks** menu, select **Reboot** to configure a the device's reboot job. To configure this job, follow these steps:

1. Specify whether the unit's configuration is saved before the reboot by checking the check box.
2. Specify the unit's reboot timeout. Default timeout is **5** minutes.
3. The **Reboot** task is now complete.
4. You can now return to configuring additional parameters for this job or other tasks to accompany this job as described in Creating a New Job.

Canceling a Job

To cancel a job, follow these steps:

1. Select the job you wish to cancel from the job list. In **Details** view, the job list is on the left side of the menu. In **Grid** view, the job list is in the center of the menu.
2. Select the **Cancel** button from the top left side of the **Jobs** menu.
3. The job has been cancelled.

Deleting a Job

To delete a job, follow these steps:

1. Select the job you wish to delete from the job list. In **Details** view, the job list is on the left side of the menu. In **Grid** view, the job list is in the center of the menu.
2. Select the **Delete** button from the top left side of the **Jobs** menu.
3. The job has been deleted and is removed from the jobs list.

Firmware

Firmware Tab

The n-Command MSP **Firmware** tab provides an interface for firmware management. To open the **Firmware** tab, select the **Open Tab** menu from the upper left-hand corner of any screen in n-Command MSP. Select **Firmware** from the drop-down menu.

Firmware is used for distribution to network devices being managed by n-Command MSP. Each device has specific firmware that can be acquired from ADTRAN. For assistance, contact your reseller or ADTRAN technical support at http://www.adtran.com.

Once the firmware is available locally, move it to the n-Command MSP server. The firmware can be held until a later time to transfer to the units through a job. Select the **New Firmware Job** button to navigate to the **Jobs** menu.

Select any of the following tasks for more information:

- Uploading Firmware to the n-Command MSP Server
- Deleting Firmware from the Server
- Updating Firmware on a Device from the Firmware Menu

	*A comma separated value (CSV) file can be exported from the **Firmware** tab listing the **File Name**, **Version**, **Size**, and **Creation Date** by selecting the **Export CSV** button from the bottom of the **Firmware** menu.*

Uploading Firmware to the n-Command MSP Server

The firmware must first be available locally before attempting to upload to the n-Command MSP server. Check with the reseller or ADTRAN technical support at http://www.adtran.com/support for the most current firmware.

To upload firmware to the server, follow these steps:

1. Navigate to the **Firmware** tab by selecting the **Open Tab** menu from the upper left-hand corner and select **Firmware** from the drop-down menu.
2. Select **Upload Firmware**.
3. Navigate to the location of the firmware you want to upload using the Open File dialog box that appears. Select the firmware file and choose **Open**.
4. Once the firmware has been transferred to the server, it appears in the **Firmware** tab window. It is now ready to be transferred to a device on the network. For more information, refer to Updating Firmware on a Device from the Firmware Menu.

NOTE	***Device Groups*** *will only display a group if firmware for that device type is currently available on the server. A group will appear as soon as new firmware is transferred to the server.*

Deleting Firmware from the Server

1. Navigate to the **Firmware** tab by selecting the **Open Tab** menu from the upper left-hand corner and select **Firmware** from the drop-down menu.
2. Select a device group from the left-hand column. The firmware available on the server (specific to the types of devices selected) will display on the right.

	***Device Groups** will only display if firmware for that device type is currently available on the server. A group will appear as soon as new firmware is transferred to the server.*

3. Select the check box next to the firmware to be removed. More than one can be selected at a time.
4. Select **Delete** at the top of the window to remove all selected firmware. The firmware is immediately removed from the server.

Updating Firmware on a Device from the Firmware Menu

Transferring firmware to a device is accomplished using a job created in the **Jobs** menu. The firmware must first exist on the n-Command MSP server before the transfer can be performed. For more information, refer to Uploading Firmware to the n-Command MSP Server. Once the firmware is available, you can navigate to the **Jobs** menu by selecting the firmware to upload, then select the **New Firmware Job** button on the top right side of the **Firmware** menu. This creates an **Upgrade Firmware** job with the **Device Group** and **New Firmware** already selected. Refer to Pushing Firmware to a Device, skipping the first two steps to continue.

Alert History and Templates

Alert History Tab

The **Alert History** tab displays all alerts for all devices on the system in a list format that is easily sorted by the column headings. To open the **Alert History** tab, select the **Open Tab** menu from the upper left-hand corner of any screen in n-Command MSP. Select **Alert History** from the drop-down list.

The number of alerts displayed on the **Alert History** tab can be limited to 10, 20, 30, 50, 100, 500, or 1000 alerts per page using the **Page Size** menu at the bottom of the page. The display settings can also be set to automatically choose the number of alerts to fit on the page (select **Auto**) or to display all alerts (select **All**). Choosing to display **All** devices could cause a delay in the amount of time it takes to refresh the screen if there are a large number of alerts. Use the navigation tools at the bottom of the page to view additional pages. By default, the alerts are displayed to automatically fit the page and are sorted by the **Time** column.

Click once on a column heading to sort the list by **Time**, **Device** name, alert **Description**, or the **Alert** level. The order can be changed from ascending to descending order with each additional click on the column heading. Double clicking on an alert entry in the grid opens the **Device Details** tab for the device.

Alert Templates

Alert templates are an easy way to apply alert settings to multiple devices at one time or to new devices as they are discovered. An alert template specifies how alerts are delivered from the devices to an administrator. This delivery method can be sent through SNMP to a monitoring agent, email sent to a valid email address, or visible from the **Alerts** widget on the main Dashboard in n-Command MSP.

To create an alert template:

1. Select **Alert Templates** from the **Open Tab** menu.
2. Enter a name for the template in the field provided and select **Add**.
3. Select the delivery method for each alert in the columns to the right under the **Alerts** heading. **E-mail** must be selected in combination with either **SNMP** or **Widget**; it cannot be selected alone. To check one delivery method for all alerts, select the check box in the column heading. This will check all the boxes below it for all alerts. Selecting **E-mail** requires additional settings under the **Email Settings** heading.

*Before alerts can be sent through SNMP, SNMP must be configured in **Settings** > **SNMP**. Refer to SNMP Settings for more information.*

*Before alerts can be sent through email, email must be configured in **Settings** > **Connection**. Refer to Connection Settings for more information.*

4. Specify the threshold for any alerts requiring limits. For example, **Low Available CFlash** defaults to **< 10**%. This can be adjusted using the up and down arrows in the **Limits** column or typing in a number to specify a value other than 10.
5. If **E-mail** is selected as a delivery option for alerts, you must also indicate the **Email Notification List** to use. From the **Email Settings** section of the **Alert Templates**, select an

email from the drop-down list. Refer to Email Settings for details about creating these entries.

5. Select the check box next to **Apply to new Devices** if you want to apply to devices when they are discovered as well. Not selecting this options indicates you want to apply the alert template only to devices currently managed by n-Command MSP.
6. Specify the **Criteria** settings. The alert template is applied to devices meeting the criteria. The criteria is set in the manner described in **Adding Criteria to Alert Templates**.
7. Once the alert template settings are configured, select **Save** to save the settings.
8. When you have created multiple alert templates, the order in which they are applied can be changed. You can drag and drop the templates within the listing on the **Alert Templates** menu and select **Save Reorder** to keep the current order. Selecting **Revert Reorder** will revert back to the previous order for the templates.

Other functions available from this menu are:

- Update Device Alert Settings
- System Alert Settings

Adding Criteria to Alert Templates

Alert templates can be applied to devices matching a specified criteria. Use the following steps to specify the criteria for an alert template:

1. From the **Alert Template** menu, be sure to select the template to configure from the list on the left. Select **Add Criteria** from the Alert Template menu. Once selected, a filter statement line is shown below the **Criteria** heading.
2. Select an attribute from the first pop-up list. The list displays all the available attributes on which to match devices, such as **Device Type**, **Location**, etc.
3. Select the action from the second pop-up list, such as **contains**, **does not contain**, **is**, or **is not**.
4. Enter the data required to complete the filter statement or select from the list if one is provide. This depends on the type of criteria selected. For instance, if you are filtering based on a device type, select **Device Type** from the first list, **is** from the second list, and a device from the third, **7100**. The devices for this alert template must match the Device Type is 7100. Once the criteria is entered, select **Save** to accept the settings.
5. Additional statements can be added by selecting the **+** (plus) sign at the beginning of the filter line, and repeating Steps 2 through 4. Likewise, statements can be removed by selecting the **-** (minus) sign next to the filter line.

Update Device Alert Settings

Alert settings can be altered for multiple devices all at one time without changing the Alert templates or creating a new one. This is accomplished through the **Update Device Alert Settings** dialog box. The alert settings specifies how alerts are delivered from the devices to an administrator. This delivery method can be sent through SNMP to a monitoring agent, email sent to a valid email address, or visible from the **Alerts** widget on the main Dashboard in n-Command MSP.

To change the alert settings and apply to devices already discovered on the network:

1. Navigate to **Open Tab** > **Alert Templates**, and select **Update Device Alert Settings** from the top of the **Alert Templates** menu.
2. Select an alert template from the drop down menu at the top of the dialog box to begin with or skip this step if one does not exist. You an always use **Default**.
3. Select the delivery method for each alert in the columns to the right. **E-mail** must be selected in combination with either **SNMP** or **Widget**; it cannot be selected alone. To check one delivery method for all alerts, select the check box in the column heading. This will check all the boxes below it for all alerts. Selecting **E-mail** requires additional settings under the **Email Settings** heading.
4. If **E-mail** is selected as a delivery option for alerts, you must also indicate the **Email Notification List** to use. From the **Email Settings** section of the **Alert Templates**, select an email from the drop-down list. Refer to Email Settings for details about creating these entries.

*Before alerts can be sent through SNMP, SNMP must be configured in **Settings** > **SNMP**. Refer to SNMP Settings for more information.*

*Before alerts can be sent through email, email must be configured in **Settings** > **Connection**. Refer to Connection Settings for more information.*

5. Select **Next**. You will now select the devices.
6. There are four options available for selecting devices to which the settings will be applied.
    - Select the **Run on ALL devices** option to apply to all discovered devices.
    - **Devices** - select the devices individually from the list, drag and drop in the Devices for Job field below.
    - **Labels** - use existing labels to select the devices. Refer to **Adding Labels** for more information.
    - **Filters** - use existing filters to select devices. Refer to **Adding Filters** for more information.
7. Select **Apply** to complete the update and apply the new alert settings to the devices selected.

System Alert Settings

There are specific alerts that can be sent pertaining to the n-Command MSP server. These are called System Alerts. Just like an alert template, the system alert settings specifies how alerts are delivered to a system administrator. This delivery method can be sent through SNMP to a monitoring agent or email to a valid email address.

To change the system alert settings:

1. Navigate to **Open Tab** > **Alert Templates**, and select **System Alert Settings** from the top of the **Alert Templates** menu.
2. Select the delivery method for each alert in the columns to the right. To check one delivery method for all alerts, select the check box in the column heading. This will check all the boxes below it for all alerts. Selecting **E-mail** requires additional settings under the **Email Settings** heading.
3. If **E-mail** is selected as a delivery option for alerts, you must also indicate the **Email Notification List** to use. From the **Email Settings** section of the **System Alert Settings** dialog box, select an email from the drop-down list. Refer to Email Settings for details about creating these entries.

*Before alerts can be sent through SNMP, SNMP must be configured in **Settings** > **SNMP**. Refer to SNMP Settings for more information.*

*Before alerts can be sent through email, email must be configured in **Settings** > **Connection**. Refer to Connection Settings for more information.*

4. Specify the threshold for any alerts requiring limits. For example, **High Disk Utilization** defaults to > **1**%. This can be adjusted using the up and down arrows in the **Limits** column or typing in a number to specify a value other than 1.
5. Select **Save** to save the settings.

Creating an Alert Email Notification

Email settings must be configured before this method can be selected for alert notifications.

To create an alert email notification, use the following steps:

1. Select **Email Settings** from the **Alert Templates** menu.
2. Enter a name for the email notification in the field provided and select **Add**.
3. Select one of the existing users from the **Notify Users** list by selecting the check box, or enter a new email address in the **Notify Other E-Mails** field. Enter multiple email addresses by typing each address on a separate line in the text field.
4. Specify whether to send alerts individually or as a summary. To send them individually, select the radio button next to **Send Alert E-mails** and specify the minimum interval in minutes. To send the alerts as a summary, select the radio button next to **Send a summary of active alerts** and specify the frequency in hours. You must select one or the other.
5. Specify the schedule to use for sending the alerts by selecting a start time, the time zone, days of the week, and a stop time. You must select a time zone before you can save the notification.
6. Select **Save** to apply all changes to the new alert email notification.

Device Details View

Device Details Tab

The **Device Details** tab is an optional menu that can be displayed by double clicking on a device from many locations throughout the software. A new tab is displayed with the device name as the heading. It provides all of the device's available information through several menus: **Summary**, **VQM Statistics**, **Backup Files**, **Alert Template**, **SIP Files**, and **Exceptions**. The **Exceptions** menu does not display if there are no **Exception** alerts on the device. If the device does not support VQM, the **VQM Statistics** tab is still available, but will appear blank. Likewise, the SIP Files tab will display, but if the device does not have SIP enabled, it will appear blank.

The title bar provides several function buttons above the chart. **Install Config** allows you to download a configuration file to the device from the server. The **Force Checkin** button forces the device to check in with the server, instead of waiting for the next refresh interval. The **Web Interface** button opens the device's Web interface in a new browser window. Selecting **Refresh VQM** initiates an update from the device and retrieves VQM statistics for the current day. Choosing an option from the **New Job** section creates a new job based on one of the following functions: **Upgrade Firmware**, **Push Config**, **Restore**, or **Reboot**. These functions are explained in more detail in Creating a New Job.

For more information about a specific menu from within the **Device Details** tab, select from the following:

- Summary Menu
- VQM Statistics Menu
- Backup Files Menu
- Alert Templates
- SIP Files
- Exceptions Menu
- Install Config Menu

Summary Menu

The **Summary** section of the **Device Details** tab provides General Information, Firmware Information, Auto-Link Information, System Usage, Exceptions, Network Information, Device Access, and VQM statistics. The only information on this screen that can be changed is the **Device Access**. Selecting the **Edit** button next to **Device Access** opens the **Device Access** dialog box, where changes can be made to the credentials. Refer to Changing or Setting Manage Access Parameters for more information.

General Info provides the name, type, platform, part number, description, serial number, hardware version, last backup time, contact interval, location, and system contact of the device. This information is all provided by the device. If no information displays for a specific entry, it is because none was provided by the device.

Firmware Info displays the running, primary, and backup firmware version. It also displays the size of the firmware files in bytes.

Auto-Link Info shows the settings for the auto-link configuration. Auto-link is the feature that allows the device to communicate with the server. This section indicates if auto-link is supported and enabled. It also displays the last time the device updated the server and when the next update is scheduled.

System Usage displays how much of the system resources (heap, nonvol, and processor) are being used by the device. This is identified by a percentage of the total resources available.

Exceptions lists the number of recent exception alerts. There are more details available for exception alerts by navigating to the **Exceptions** menu in the **Device Details** tab. Refer to Exceptions Menu for more information.

Network Info displays the domain naming system (DNS) name and the IP address of the device.

Device Access shows the name for the set of parameters being used to access the device. It also shows the name of the access

credentials, IP address settings, port number, and the method used.

VQM is an optional section of the **Summary** menu. Not all devices have voice quality monitoring (VQM) statistics. If available, **VQM** statistics are provided in a summary graph at the bottom of the screen displaying the **MOS LQ** and **Call Quality**. The data can be filtered to show only a specific interface or to show a summary of all calls. To change the filter, select the down arrow in the upper right portion of the VQM summary section. The menu that appears lists the available interfaces and also the **Summary** option. Select one of the options from the list.

The time frames shown cover three different intervals: 1 hour, 12 hours, and 1 day. More details are provided for each interval in a tool tip by moving the mouse over the bar on the graph. For the **MOS LQ** graph, the pop-up window displays the number of calls and the latency queueing (LQ) average. For the **Call Quality** graph, the tool tip displays the number of calls and the quality represented by each color bar. For instance, green shows **Excellent** call quality and blue shows **Good** call quality. To review the data in greater detail, double click a bar in the graph. This brings up the detailed **VQM Statistics** menu, filtering the data based on the bar graph selected. If the bar graph you selected displayed only VLAN 2 calls, then the resulting **VQM Statistics** graph shows only data for calls on VLAN 2 calls. Refer to VQM Statistics Menu for more information.

VQM Statistics Menu

Voice quality monitoring (VQM) allows real time passive Voice over IP (VoIP) quality measurements to be taken on all Realtime Transport Protocol (RTP) voice streams transmitted through an AOS device. The VQM statistics gathered by the AOS device are shared with the n-Command® MSP server using the VQM reporter. The reporter must be enabled on the AOS device before n-Command MSP can aggregate the VQM statistics gathered by the AOS device. Configuring the VQM reporter is done through the command line interface (CLI) on the AOS device, and consists of creating the reporter, configuring the parameters of the reporter, and viewing the reporter statistics. The reporter must be configured before n-Command MSP will gather VQM statistics. VQM reporter configuration instructions are outlined in the guide *Configuring VQM Reporter for AOS and n-Command MSP*, available from ADTRAN's Support Forum at http://supportforums.adtran.com.

The **VQM Statistics** menu has two methods for viewing voice data. The first is a line chart that displays mean opinion score listening quality (MOS LQ) averages, individual voice streams, or a combination of the two. The second section is the individual call detail grid. To switch from one view to another, select the appropriate icon on the bottom left of the graph. Move the mouse over the icon to display a tool tip describing the view option. The individual call detail grid section is toggled on or off by selecting the last of the four view option icons.

More information is provided for interpreting VQM statistics in *Configuring Voice Quality Monitoring (VQM) in AOS*, available from ADTRAN's Support Forum at: http://supportforums.adtran.com.

Line Graph

The line graph can display the averages of one interface or the average of all interfaces on the device. Select or deselect the interfaces using the check boxes to the left of the line graph. Not all of the listed interfaces will have voice data to report.

The refresh rate can be changed by selecting the **Chart Options** from the lower left corner of the screen. The refresh rate only applies to the chart when you are viewing the current day. Make a selection from the drop-down menu.

A 2-week interval is shown on the bottom graph. To zoom in on a smaller time period and display it in detail on the top graph, click and drag the sliders to include the time frame. The tool tips display a start and end time. The date can be changed by selecting the pop-up menu from the lower right corner next to **Jump to Day**. Select a date from the list to apply it to the line graph.

Individual Call Detail Grid

The individual call detail grid lists every call individually and can be filtered by selecting the **Add Filter** menu option at the bottom of the grid. Apply a filter in the same manner described in the section Adding a Filter to a List. The columns can be hidden or revealed by selecting the **Manage Columns** menu option at the bottom of the grid, as discussed in Manage List Columns.

Double click a row in the grid to display individual call details. The line graph disappears, and a new menu is displayed. The new menu lists several collapsed categories, all of which provide details of the call. Select the category to expand the details. Select the category again to collapse it. Multiple categories can be opened at one time.

Backup Files Menu

The **Backup Files** section of the **Device Details** tab provides a list of backup points to use for restoring the device configuration. The backup points are defined on the device itself as to when they are created. To review a backup file, select a backup point from the list on the left. A list appears, providing the **Path**, **Name**, **Size**, and date **Modified On** for each backup file. Each file can be downloaded locally by double clicking the file name and selecting a location in which to save it. To sort the list, click on the column heading. The order changes from ascending to descending with each additional click.

Individual Device Alert Settings

The method used to deliver alerts can be altered on a per device basis. From the **Device Details** tab, select the **Alert Templates** button to display the current alert settings.

1. To change the way an alert is handled, select the check box in the columns under the delivery method **SNMP**, **Widget**, or **E-mail**. To change method for all the alerts, you can select the check box in the column heading and it will apply the change across all alert types. **E-mail** cannot be selected as the only delivery method. You must select either **Widget** or **SNMP** first in order to also select **E-mail**.
2. After making changes to the alert settings, select **Apply** to save the changes. The changes you made will apply only to this particular device.

If you are choosing email for any alerts, this method requires also selecting an email address from the drop-down list under **Email Settings** (located at the bottom of the menu). These addresses are populated from the **Alert Templates** menu accessible from the **Open Tab** menu.

*Before alerts can be sent through SNMP, SNMP must be configured in **Settings** > **SNMP**. Refer to SNMP Settings for more information.*

*Before alerts can be sent through email, email must be configured in **Settings** > **Connection**. Refer to Connection Settings for more information.*

SIP Files Menu

The **SIP Files** section of the **Device Details** tab provides a list of packet capture (PCAP) files received for the device. This information is available only if SIP is enabled on the device.

The PCASH settings must also be configured before SIP traffic PCAP files will be received. Refer to PCASH Settings for more information.

To sort the list by a specific column, click on the column heading. The order changes from ascending to descending with each additional click. The PCAP list has many of the same tools available on the other menus in n-Command MSP, such as **CSV**, **Refresh**, **Filter,** and **Columns**. The number of PCAP files displayed can be limited to 20, 30, 50, 100, 500, or 1000 devices per page using the **Page Size** menu at the bottom of the page. The display settings can also be set to automatically choose the number of files that will fit on the page (select **Auto**) or display all files (select **All**). If there are a large number of PCAP files to display, choosing **All** files could cause a delay in the amount of time it takes to refresh the screen. Use the navigation tools at the bottom of the page to view additional pages. By default, the files displayed will automatically fit the page and are sorted by the **Begin** time column.

To view a ladder diagram displaying the SIP call sequence for a specific file, select a PCAP entry from the list and double click on the entry. A new tab opens with the name of the file as the header. From this tab, each transaction is displayed and the exact time it occurred. You can also download the file locally by selecting the **Download pcap file** button in the upper right corner and specifying a location in which to save it.

Exceptions Menu

The **Exceptions** section of the **Device Details** tab provides more information about each **Exception** alert active on the device. The name of the report, size, and date it was created are all displayed in this section. Double click on the report name to download the file locally and review the contents.

Installing a Configuration File

The **Install Config** feature is available from the **Device Details** tab. It provides a method for downloading a configuration file to a specific unit. The configuration file can be created prior to installing on a unit that has already been deployed and is currently being managed by n-Command MSP.

To install a configuration file, follow these steps:

1. Select **Install Config** from the menu options on the **Device Details** tab for the specific device.
2. Select the appropriate configuration file from the local directory or network location.
3. Select **Open** to upload the file.

Settings

Settings Menu

The **Settings** menu is located in the top right corner of the n-Command MSP menu, and provides quick access to manage settings and viewing preferences. By selecting the **Settings** menu, the following options are available in the drop-down list:

- Authentication Settings
- Ignore Devices
- License Information
- Log Settings
- Login Banner
- Mail Settings
- Message Log
- PCASH Settings
- Reverse DNS
- SNMP Settings
- System Backup
- System Restart
- System Updates
- Users
- VQM Statistics Export

NOTE	*With release 5.1 of n-Command MSP, the **Network Settings** menu option was moved to the Administration Dashboard. Refer to Network Settings and Administration Dashboard for more information.*

Authentication Settings

The **Authentication Settings**, available from the **Settings** menu, indicate the method to use for user authentication, such as Local, Radius, LDAP, or Active Directory. Each method requires specific settings be provided in order to authenticate users and allow them access to the n-Command MSP server. After an authentication type is selected, the dialog box displays the appropriate fields to populate for that method. Use the following instructions for the method that best meets your needs:

- Local
- RADIUS
- LDAP
- Active Directory

Once changes have been made to the settings in the dialog box, select **Apply** to save and exit the menu. Select **Cancel** to exit without making any changes.

Local Authentication

After selecting the **Local** authentication method, select **Apply** to save and exit the menu. Select **Cancel** to exit without making any changes. Selecting Local authentication allows users to login using the credentials stored on the local n-Command MSP server. These settings are configured from the **Users** tab.

*Changing to another authentication method after using the **Local** authentication method does not erase the local users. If a user has the same user name in the local system as another authentication method (such as LDAP or Active Directory), the local user password will no longer authenticate locally. Take this into consideration when changing back to **Local** authentication from another method. The user password will have to be changed by the administrator to allow the user to login again.*

Radius Authentication

After selecting the RADIUS authentication method, you will need to provide the following information:

1. Assign the **authentication type** as either **CHAP** or **PAP**.
2. Enter the **Authentication Server** address.
3. Enter the **server Port** (the default is 1812).
4. Select a number of **Server Retries**.
5. Enter the **shared key**. (The shared key is the key received from the server administrator.)
6. Enter the shared key again by entering it in the **Verify Shared Key** field.

Once changes have been made to the settings in the dialog box, select **Apply** to save and exit the menu. Select **Cancel** to exit without making any changes.

LDAP Authentication

After selecting the LDAP authentication method, you will need to provide the following information:

1. Assign the authentication type as **Simple**, **Digest MD5**, or **Kerberos**.

	Simple authentication type is NOT recommended since it does not encrypt passwords.

2. Enter the **Authentication Server** address.
3. Enter the **Server Port** (the default is 389).
4. Enter the **Security Domain** (for example, **corp.mycompany.com**).
5. In the **User Base DN** field, specify the DN of the root location to begin an LDAP search for a user record. This attribute is used by n-Command MSP to locate user information.

   If you select **Bind User Base DN to Security Domain**, the DN field will populate with domain components (**dc**) based on the defined security domain.

   You can add common name (**cn**), user identification (**uid**), and organizational unit (**ou**) attributes to the **User Base DN** field after it is populated or enter the information manually by clicking in the field (for example, **uid=%user%,ou=employee,dc=corp,dc=mycompany,dc=com**).

6. Specify an attribute filter to use in locating a user record in the **User Filter** field. This filter is used to find a user record from the **User Base DN**. It is common to use the user name attribute for this filter, but not required (for example, **uid=%user%**). (The **%user%** escape sequence will be replaced by the user login at the time of authentication.) This field also allows the **cn**, **uid**, and **ou** attributes to be added.

Once changes have been made in the dialog box, select **Apply** to save and exit the menu. You can select **Cancel** to exit without making any changes.

Next, set the user permissions as described in the following section:

Setting User Permissions for LDAP or Active Directory Authentication

Active Directory Authentication

After selecting the **Active Directory** authentication method, you will need to provide the following information:

1. Assign the authentication type **Kerberos**.
2. Enter the **Authentication Server** address.
3. Enter the **Server Port** (the default is 389).
4. Enter the **Security Domain** (for example, **CORP.MYCOMPANY.COM**).
5. Specify the DN in the **User Base DN** field. n-Command MSP uses this attribute to locate user information.

   If you select **Bind User Base DN to Security Domain**, the DN field will populate with domain components (**dc**) based on the defined security domain.

   You can add common name (**cn**), user identification (**uid**), and organizational unit (**ou**) attributes to the **User Base DN** field after it is populated or enter the information manually by clicking in the field (for example, **uid=%user%,ou=employee,dc=corp,dc=mycompany,dc=com**).
6. Specify an attribute filter to use in locating a user record in the **User Filter** field. This filter is used to find a user record from the **User Base DN**. It is common to use the user name attribute for this filter, but not required (for example, **sAMAccountName=%user%**). (The **%user%** escape sequence will be replaced by the user login at the time of authentication.) This field also allows the **cn**, **uid**, and **ou** attributes to be added.

Once changes have been made in the dialog box, select **Apply** to save and exit the menu. You can select **Cancel** to exit without making any changes.

Next, set the user permissions as described in the following section:

Setting User Permissions for LDAP or Active Directory Authentication

Setting User Permissions for LDAP or Active Directory Authentication

After selecting either **LDAP** or **Active Directory** authentication method, you will need to set the user permissions in order for the n-Command® MSP permissions to be retrieved correctly. This function should be performed by an administrator familiar with the LDAP or Active Directory methods used in your network.

Use one of the following two methods to set the user permissions in n-Command MSP:

1. Add the **adtranMSPPermissions** attribute to the user record. The **adtranMSPPermissions** defines permissions over multiple values or lists them in a comma-separated list. The permission values must be selected from the list in the table below.
2. Add the **memberOf** attribute to the user entry. The **memberOf** attribute contains multiple values and is not case sensitive. Each value of the **memberOf** attribute can only contain the DN of a group record that represents an n-Command MSP permission. The group CN must be one of the values listed in the table below. The **memberOf** attribute may be generated automatically by your LDAP server when a user record is assigned to a group on the system.

Attribute	User Permission
adtranMSPAll	All permissions
adtranMSPRestore	Restore device configurations
adtranMSPReboot	Reboot devices
adtranMSPPushConfig	Push configurations to devices
adtranMSPPushFirmware	Push firmware to devices
adtranMSPDiscover	Discover devices on the network
adtranMSPPurgeExcept	Purge exceptions on devices
adtranMSPManageUser	Manage users on the n-Command server
adtranMSPManageServer	Manage the n-Command server

	If a user is not defined with permissions as described above, they will be able to log into the n-Command MSP server, but will not have permission to perform any actions.

Ignore Devices

The **Ignore Devices** selection of the **Settings** menu provides a dialog box to specify a serial numbers for specific devices on the network to ignore. Once a device is added to the list, it is ignored every time n-Command MSP updates until it is removed from the list. To add a device to the **Ignore Devices** list, use the following steps:

1. Select **New** from the dialog box.
2. Enter the serial number, adding any comments as necessary.
3. Select **Save**.

License Information

The banner across the top of the screen displays the license information for the current installation of
n-Command MSP. This license information changes color depending on the current status. It displays green if the license is currently valid, yellow if you are within 30 days of expiration of the license period, and red if the license has expired.

The **License Information** section of the **Settings** menu displays a dialog box that enables you to view or update your n-Command MSP license information. New licenses can be entered from this dialog box, but you must first register the product at http://www.adtran.com. Only registered users of the ADTRAN support website can register products and generate a license certificate. Use the following steps to complete the licensing process:

1. Select **License Information** from the **Settings** menu.
2. Select **Generate Challenge Key** to display a challenge key. Leave this dialog box open because you will return to it in Step 11.
3. Open another browser window and navigate to http://www.adtran.com.
4. Select **Support** > **Product Registration** > **Register a product** from the drop-down menu.
5. Log in using your ADTRAN user name and password. If you have not previously registered as a user at ADTRAN's support website, select the **Register an account** link, and follow the prompts.
6. If this is your first time registering your product, you must enter the n-Command MSP serial number in the field provided under **Product Registration - Step 1**, and select **Continue**. (If you have previously registered your product, it appears in the **Registered Product** list and you can proceed to Step 8.)

NOTE	*The n-Command MSP serial number appears in two locations. One location is in the License Entry dialog box from within the n-Command MSP. The other location is on a pull-out tab labeled **EST**, located on the front of the server hardware and is titled **Service Tag**.*

7. Select **Continue Product Registration** from **Product Registration - Step 2**. A final page displays which confirms the product registration is complete.
8. Select **NCommand MSP Licensing** from any of the n-Command MSP products listed in the **Registered Products** list.
9. Select **Get License Key** from the same line as the n-Command MSP server you are registering.

10. Enter the challenge key from the n-Command MSP software that you generated in Step 2 (you can copy and paste the string) and select **Generate License Key**. A license certificate is generated and emailed to the registered user. Save the file containing the license certificate. You will upload it to the n-Command MSP server in the next step.
11. Return to the n-Command MSP software. Select **Import License Certificate** from the **License Entry** dialog box, and locate the saved email attachment. It may take a few minutes to import.
12. Select **Update** to save the new information. You have successfully registered and licensed your software. Successful licensing is confirmed by the population of a **License Expiration Date**, **Feature Limit**, and **Current Device Count** displayed in the **License Entry** dialog box.

Log Settings

The **Log Settings** selection of the **Settings** menu displays a dialog box that lists all log configurations. New log entries can be created or existing configurations can be edited or deleted from this dialog box. Select a topic for more information.

- Creating a New Log Entry
- Editing a Log Entry's Notification Type
- Deleting a Log Entry

Log Settings can have a negative effect on unit memory if too many items are logged. Do not make any changes to Log Settings unless prompted by Technical Support or your network administrator.

Creating a New Log Entry

To create a new log entry, follow these steps:

1. Select the **New** tab at the top left corner of the **Log Settings** dialog box.
2. Enter the name of the log in the appropriate field.
3. Specify the notification type from the drop-down menu.
4. Select **Cancel** if you do not wish to add the log.
5. Select **Add** to add the log to the **Log Settings** list.
6. Select **Save** before exiting the **Log Settings** menu.
7. Exit the **Log Settings** menu by selecting the **X** in the top right corner of the box.

	Log Settings can have a negative effect on unit memory if too many items are logged. Do not make any changes to Log Settings unless prompted by Technical Support or your network administrator.

Editing a Log Entry Notification Type

The log entry's notification is the only log parameter that can be edited from the **Log Settings** dialog box. To edit a log entry notification type, follow these steps:

1. Select the log entry to edit by highlighting the selection.
2. Select the appropriate notification type (**Info**, **Warn**, **Debug**, **Trace**, or **Error**).
3. Select **Cancel** if you do not wish to change the notification type.
4. Select **Save** to save the changes made to the log entry.
5. Exit the **Log Settings** menu by selecting the **X** in the top right corner of the box.

	Log Settings can have a negative effect on unit memory if too many items are logged. Do not make any changes to Log Settings unless prompted by Technical Support or your network administrator.

Deleting a Log Entry

To delete a log entry from the **Log Settings** list, follow these steps:

1. Select the log entry to delete by highlighting the selection.
2. Select **Delete** from the top left corner of the menu.
3. Select **Save** to save the new list.
4. Exit the **Log Settings** menu by selecting the **X** in the top right corner of the box.

Log Settings can have a negative effect on unit memory if too many items are logged. Do not make any changes to Log Settings unless prompted by Technical Support or your network administrator.

Login Banner Settings

The **Login Banner** option of the **Settings** menu allows you to add or change the message displayed before logging into the system. Enter the message in the box provided and select **Save** to accept the changes, or select **Cancel** to exit without making any changes.

Mail Settings

The Simple Mail Transfer Protocol (SMTP) configuration settings are accessed from the **Mail Settings** option on the **Settings** menu. From this dialog box, you can review the **Sending User**, **Host**, and **Port** settings of the n-Command MSP server. To make changes, enter the information in the fields provided and select **Save**. A test message can also be sent to confirm the settings are correct. Enter an email address in the **To Address** field and select **Test**. A test message is sent using the defined SMTP parameters.

Message Log

The **Message Log** selection of the **Settings** menu displays a list of messages generated by the server. The log also displays the time the message was logged and the type of message sent. When a user performs an action in the system, it generates an entry in the message log. The types of messages that can be captured are success, error, and warning.

PCASH Settings

The **PCASH Settings** selection of the **Settings** menu displays a dialog box to enter the user name and password for the Packet Capture Archival Server HTTP (PCASH). This enables n-Command MSP to communicate with the PCASH to receive SIP traffic packet captures (PCAPs) from AOS devices. This information is used to populate the SIP ladder diagram in n-Command MSP, available from the **Device Detail** tab. SIP must be enabled on the AOS device in order for PCAPs to be sent.

Reverse DNS

The **Reverse DNS** option of the **Settings** menu allows you to enable reverse domain naming system (DNS) lookup. If this option is enabled, when a device checks in with the n-Command MSP server, a reverse DNS lookup is performed on the IPv4 address. If a host name is associated with the IPv4 address, n-Command MSP will use the fully qualified domain name (FQDN) instead of the IPv4 address. Select the check box next to **Enable Reverse DNS** to enable, and select **Save**.

Select **Cancel** to exit the dialog box without performing any of these functions.

SNMP Settings

The **SNMP Settings** selection of the **Settings** menu displays a dialog box that lists the Simple Network Management Protocol (SNMP) settings for the n-Command MSP server. Use this dialog box to configure or edit the SNMP trap settings.

1. Select **SNMP Settings** from the **Settings** menu.
2. Enter the management server IP address in the **Host 1** field. The address should be for the server that will receive the SNMP traps.
3. Enter the **Port** number to use on the server. The default port is **162**.
4. Enter the SNMP community string to include with the trap in the **Community** field.
5. Select which SNMP version to use. Choose either **v1** or **v2c** (even though version 3 appears in the drop-down menu, it is not currently supported).
6. Select the **Inform** check box if you want to issue version 2 inform messages instead of version 2 traps. If you select inform messages, the management station is required to send an acknowledgement message. The system resends the inform message until it is acknowledged or the maximum retries threshold is reached. The **Timeout** value and number of **Retries** can only be set once the **Inform** option is selected. The **Timeout** is entered as milliseconds and represents the amount of time the system waits before resending. The **Retries** value is the number of times the system will retry sending the inform message before the operation fails.
7. Enable traps for a specific alert by selecting the check box beside the alert. Use the scroll bar to move up and down the list. An **Enable All** and **Disable All** button is provided to make selecting all alerts or deselecting all alerts easier. The alerts are listed in groupings based on their associations. For example, the first six alerts listed correspond to the **Device Alerts** module on the Dashboard. The next six are all SNMP alerts generated by the devices. The next six alerts pertain to the n-Command MSP server conditions and correspond to the **System Performance** module on the Dashboard.
8. Once all settings are finalized, select **Save**.

System Backup

The **System Backup** selection of the **Settings** menu enables you to view available system backups, create a backup schedule, configure the remote FTP server settings, and test the remote server settings.

Viewing the Available System Backups

Available system backups are listed on the **Backups** tab of the **System Backup** dialog box. You can place the cursor over a backup entry to view the full details of the backup.

Creating a Backup Schedule

To create a backup schedule, select **Backup Schedule** from the **System Backup** dialog box.

1. Select the days of the week for the system backups to run.
2. Select a time of day using the hour and minutes fields.
3. Select **Save** to save these settings.

Configuring and Testing the Remote FTP Server Settings

The remote settings are used to automatically upload the system backup files to a remote FTP server. Remote settings can be configured by selecting the **Remote Settings** tab of the **System Backup** dialog box. Once selected, follow these steps to configure and test the remote server settings:

1. Enter the remote FTP server IP address in the **FTP Server** field.
2. Enter the directory location in the **FTP Directory** field.
3. Enter the user name in the **FTP Username** field.
4. Enter the password in the **FTP Password** field.
5. Select **Test** to test the remote connection.
6. Select **Save** to save these settings.

System Restart

The **System Restart** option of the **Settings** menu allows you to restart the n-Command MSP application. Select **Restart** to restart the n-Command MSP application service without powering down the server.

Select **Cancel** to exit the dialog box without performing any of these functions.

System Updates

The **System Updates** selection of the **Settings** menu provides access to available updates for the n-Command MSP software. From this dialog box, you can view the system updates available for your server and current release notes. You can choose to install the update from the released versions available online or choose a file stored locally on your own computer.

To install an update, follow these steps:

1. Select **Settings** from the upper right portion of any menu.
2. Select **System Updates** from the **Settings** list.
3. Select an update from the list and choose the **Install Update** button.

To upload a file stored locally, follow these steps:

1. Select **Settings** from the upper right portion of any menu.
2. Select **System Updates** from the **Settings** list.
3. Choose **Browse** to locate the file on your local system.
4. Choose the **Upload File** button.
5. Once the file is uploaded, a dialog box prompts you to continue. Select **Apply** to install the update to your server and reboot the system. Select **Cancel** to cancel this operation.

VQM Statistics Export

The VQM data for all devices on the n-Command MSP system can be exported to a comma-delimited file (.csv) at a specified scheduled time. The schedule can be exported daily at the same time, or a single export can be requested. The exported file contains all VQM data received during the previous day. When exported, the .csv file is compressed via gzip and transferred to the destination specified. Select **VQM Statistics Export** from the **Settings** tab.

To specify a daily schedule, select the **Schedule Export** tab from the **VQM Statistics Export** dialog box. Use the following steps to configure the schedule:

1. Select the time for the system to pull the records from the **New Schedule** field. ADTRAN recommends you select a time after 12:30 a.m. in order to include all records from the previous day. You should also consider off-peak times, if this action requires pulling a large amount of data to avoid network traffic issues.
2. Specify the remote server to store the exported files using FTP. Enter the server IP address, directory location, user name, and password in the appropriate fields under **Remote Destination**.
3. Select **Save** to save the new schedule. n-Command MSP will export the VQM statistics daily, at the time specified.

Tips:

- Select **Test Connection** to make sure the ftp server information is correct.
- To disable the scheduled export, remove the server information from the **Remote Destination** fields in the **VQM Statistics Export** dialog box and select **Save**.

To request files from a previous 24-hour time period, select the **Submit Export** tab from the **VQM Statistics Export** dialog box. Use the following steps to request the data:

1. Select the **Export Date** from the calendar field to specify a 24-hour time period of data to export.
2. Specify the remote server to store the exported files using FTP. Enter the server IP address, directory location, user name, and password in the appropriate fields under **Remote Destination**.

3. Select **Submit** to complete the process and request the export file.

Tips:

- Select **Test Connection** to make sure the FTP server information is correct.
- The file naming scheme is: **callhistoryexport_serial#-version-date.csv.gz**. **serial#** is the n-Command MSP server serial number, **version** is the version of n-Command MSP running on the server, and **date** is the date the export was submitted. Previously exported files will be overwritten if a new export is issued using the same file name.

	Only one export process can run at a time.

Users

Users Tab

The n-Command MSP **Users** tab provides network administrators with the ability to manage the users of the system. Administrators can create new users, update user's settings and contact information, and delete users from the system from a single screen.

To open the **Users** tab, select the **Settings** menu from the top right corner. Select **Users** from the drop-down menu.

For more information about specific tasks, select from the following list:

- Adding a New User
- Changing a User's Password
- Editing User Settings
- Deleting a User

Adding a New User

Prior to adding a new user, you should have the following user information readily accessible:

- User Name
- User Password
- User Email Address
- User Contact Name
- User's Office and Mobile Phone Numbers
- User Permissions

To add a new user to the system, follow these steps:

1. Select **Add User** on the top left corner of the menu.
2. Complete the required fields under the **Account Settings** heading:

    - The **User Name** is the name used for logging into the system.
    - The **Password** is the password used to access the system. The password must be verified.
    - The **Email Address** is the user's contact email address.
    - By default, the account is marked as **Active**. You will need to change this if you do not want the account to be active.

3. Complete the necessary fields under the **Contact Information** heading. Enter the user's **Name**, **Office Phone Number**, and **Mobile Phone Number**. These fields are not required, but may be beneficial.
4. Enable the user's permissions under the **Job/User Permissions** heading. You will need to know what this particular user will be allowed to do in the system.

    - **Restore Configurations** allows users to create jobs to restore monitored units to previous configurations.
    - **Restart Devices** allows users to create jobs to reboot monitored units.
    - **Push Configurations** allows users to create jobs to load configurations on monitored units.
    - **Discover Devices** allows users to discover, connect, and manage units monitored by the server.

- **User Management** allows users access to the **Users Tab**, and gives permission to edit user configurations.

For more information on specific jobs, refer to the **Jobs** tab.

5. When all required fields are complete, and user permissions have been enabled, select **Save User** from the top right corner of the menu. Close the new user tab and select the **Users** tab. The newly added user appears in the user list.

Changing a User's Password

To change a user's password, follow these steps:

1. Select the user's name from the user list and double click on the link.
2. The user's information appears full screen. To edit the password information, select **Edit User** at the top right corner of the menu.
3. Under the **Account Settings** heading, delete the old password from the **Password** field and enter the new one in its place.
4. Enter the new password in the **Verify Password** field.
5. After the new password has been entered and verified, select **Save User** from the top right corner of the menu.

Editing User Settings

To edit a user's settings, follow these steps:

1. Select the user's name from the user list. Double click on this user entry.
2. The user's information appears in full screen. To edit the user information, select the **Edit User** button at the top right corner of the menu.
3. Edit the necessary information. Only the network administrator can edit the **Job/User Permissions**. The **Password**, **Email Address**, and **Contact Information** can be edited by anyone with access to the **Users** tab.
4. When the necessary information has been changed and is correct, select **Save User** from the top right corner of the menu.

	*User settings for the currently logged-in user can be edited at any time by selecting **Edit account** at the top right corner of the n-Command® MSP window. For more information about the **Edit account** tab, refer to n-Command MSP Quick Reference.*

Deleting a User

To delete a user, follow these steps:

1. Select the user to be deleted from the user list.
2. Select **Delete** from the top left corner of the menu.

	*There is no verification prompt for deleting a user. Once the **Delete** button is selected, the user is removed from the system.*

	Any user except the administrator can be deleted from the system.

Quick Reference

n-Command MSP Quick Reference

There are many features of the n-Command MSP software common to many of the work areas. For more information about these features, select one of the following:

- Settings menu
- Help menu
- Edit Account menu
- Logout menu
- Dashboard Icons
- Add Filters
- Manage Columns
- CSV Format Export

Help Menu

Selecting the **Help** menu displays a drop-down menu that provides access to online support and the **About n-Command MSP** dialog box. Online support is provided through Help files and topics. Once you have selected **Online Support** from the **Help** menu, you can navigate through the Help topics from the **Contents** menu, **Index**, or conduct a search.

About n-Command MSP

The **About n-Command MSP** selection of the **Help** menu provides an overview of the version of n-Command MSP you are using. From this dialog box, you can view the following information:

- Serial Number
- Server Version
- Client Version
- Build Date

From this menu, you can also check for updates to your version of n-Command MSP by selecting the **System Updates** hyperlink (if available), or view any release notes for this product by selecting the **Release Notes** hyperlink. The **System Updates** link opens a new browser window from which you can apply the latest available update file, or you can upload an ADTRAN-supplied update file and apply it to your system. The **Release Notes** link opens a new browser window that displays relevant release notes for n-Command MSP.

Edit Account Menu

Selecting the **Edit account** menu opens a window to edit the user account of the currently logged-in user. The window opens and displays the user's information. To edit this information, select the **Edit User** button at the top right side of the window. You can then edit the information as necessary, and select **Save User** when your edits are complete.

Logout Menu

The **Logout** menu allows you to safely exit the n-Command MSP software. When you select this option, you are automatically logged off the system, and returned to the login screen.

Dashboard Icons

There are three main icons displayed on every dashboard module: **arrow**, **X**, and **wrench**. Each icon is described below.

Arrow Icon
The **arrow** icon is located to the left of the **X** icon at the top right side of each dashboard module. Selecting the **arrow** icons maximizes or minimizes the dashboard module.

X Icon
The **X** icon is located at the top right side of each dashboard module. Selecting the **X** icon on a dashboard module closes that dashboard module.

Wrench Icon
The **wrench** icon is located at the bottom right side of each dashboard module. Selecting the **wrench** icon displays configurable parameters for the display of the dashboard module. The icon enables you to choose how the information is displayed on each dashboard module.

For more information about dashboard modules, refer to Dashboard Tab.

Adding a Filter to a List

Anywhere in the n-Command MSP software that there is a columned list of information, a **Filter** button is available at the bottom right of the list. Selecting this button enables you to select a previously saved filter from the list and limit how much data is displayed in the list. The information available for filtering varies by list. For example, information for listed devices will not be the same as information listed for voice quality monitoring (VQM), but the method for customizing the list is the same.

If a filter is already saved, select the filter name from the list to apply it to the current menu. If the filter has not been created yet, use the following steps to apply a filter to the list using the **Add Filter** option:

1. Select **Add Filter** from the menu. Once selected, a filter statement line is shown above the list.
2. Select a field from the first drop-down menu. The list displays all the data available depending on the menu you are reviewing.
3. Select the criteria to match, such as **contains**, **less than**, **is not equal to**, etc.
4. Enter the data required to complete the filter statement. For instance, if you are filtering based on a date, enter a date in the required field. Once the criteria is entered, select **Search** to apply the filter.
5. Additional statements can be added by selecting the **+** (plus) sign at the beginning of the filter line, and repeating Steps 2 through 4. Likewise, statements can be removed by selecting the **-** (minus) sign next to the filter line.

Managing Columns

n-Command MSP provides a **Columns** management option in areas of the software with lists of data. These lists display multiple columns of information, such as host name, firmware, serial number, user names, etc. Anywhere in the software that has a columned list of information, there is a **Columns** button in the bottom right side of the list. Selecting this button allows you to choose which set of information is displayed in the list. Optional information varies by list, as information for devices will not be the same as information listed for users, but the method for customizing the list is the same.

To customize the list using the **Columns** menu, follow these steps:

1. Select the **Columns** button at the bottom of the list. Once selected, all the information that can be displayed in the list is shown in a pop-up menu.
2. Select which options you would like to view in the list by checking the check box next to the item.
3. Deselect any options you do not want to view in the list by removing the check from the check box next to the item.
4. When you have selected what you want to be displayed in the list, select the **X** at the top right of the **Columns** pop-up menu.
5. Your list is now customized to your preference.

CSV Format Export

n-Command MSP provides you with the ability to export list information in comma separated value (CSV) file format. This feature is available in any area of the software that contains a columned list (for example, **Users** tab, **Devices** tab, etc.).

To export list information in a CSV format, follow these steps:

1. Select the **CSV** button at the bottom left corner of the list.
2. In the dialog box that appears, specify the file name in the appropriate field, and specify your save location.
3. Select **Save**.
4. Your list information is exported in a CSV file to the location you specified.

	*If multiple pages of information are displayed (i.e., on the **Devices** tab) only the current page will be exported. To export all devices being managed by the system from the **Devices** tab, be sure to change the **Page Size** to **All** before exporting to a CSV file.*

F.A.Q.

n-Command MSP Frequently Asked Questions

Select from the following topics for more information:

- Why don't I have a Users tab?
- Why can't I edit a user's jobs and permissions?

Why don't I have a Users tab?

Not all users have access to other user's information. If you do not have a **Users** tab, your profile does not have permission to access other user's profiles. The administrator always has access to create, edit, and delete user's profiles. If you require this access, contact your administrator.

Why can't I edit a user's jobs and permissions?

You may have only limited access to other user's profiles. Based on the permission of your profile, you may or may not be able to edit the jobs and permissions of other users. The network administrator always has permission to edit all user's jobs and permissions. If you require the ability to edit the jobs and permissions of other users, contact your network administrator.